Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2011 Proceedings

European Conference on Information Systems (ECIS)

10-6-2011

TAXONOMY OF TECHNOLOGICAL IT OUTSOURCING RISKS: SUPPORT FOR RISK IDENTIFICATION AND QUANTIFICATION

Tobias Ackermann

André Miede

Peter Buxmann

Ralf Steinmetz

TAXONOMY OF TECHNOLOGICAL IT OUTSOURCING RISKS: SUPPORT FOR RISK IDENTIFICATION AND QUANTIFICATION

Ackermann, Tobias, Technische Universität Darmstadt & CASED, Hochschulstraße 1, 64289 Darmstadt, Germany, tobias.ackermann@cased.de

Miede, André, Technische Universität Darmstadt, Rundeturmstr. 10, 64283 Darmstadt, Germany, andre.miede@kom.tu-darmstadt.de

Buxmann, Peter, Technische Universität Darmstadt & CASED, Hochschulstraße 1, 64289 Darmstadt, Germany, peter.buxmann@cased.de

Steinmetz, Ralf, Technische Universität Darmstadt, Rundeturmstr. 10, 64283 Darmstadt, Germany, ralf.steinmetz@kom.tu-darmstadt.de

Abstract

The past decade has seen an increasing interest in IT outsourcing as it promises companies many economic benefits. In recent years, IT paradigms, such as Software-as-a-Service or Cloud Computing using third-party services, are increasingly adopted. Current studies show that IT security and data privacy are the dominant factors affecting the perceived risk of IT outsourcing. Therefore, we explicitly focus on determining the technological risks related to IT security and quality of service characteristics associated with IT outsourcing. We conducted an extensive literature review, and thoroughly document the process in order to reach high validity and reliability. 149 papers have been evaluated based on a review of the whole content and out of the finally relevant 68 papers, we extracted 757 risk items. Using a successive refinement approach, which involved reduction of similar items and iterative re-grouping, we establish a taxonomy with nine risk categories for the final 70 technological risk items. Moreover, we describe how the taxonomy can be used to support the first two phases of the IT risk management process: risk identification and quantification. Therefore, for each item, we give parameters relevant for using them in an existing mathematical risk quantification model.

Keywords: IT outsourcing, IT risk management, taxonomy, risks, IT security, quality of service, literature review.

1 Introduction

The past decade has seen an increasing interest in IT outsourcing (ITO) as it promises companies many economic benefits, such as cost reduction, the possibility to focus on core capabilities, access to the providers' expertise and skills, improved business and process performance, as well as better scalability (Lacity, Khan and Willcocks, 2009). Another advantage, compared to in-house data processing, is that most providers charge on a pay-per-use basis which means that the customers do not have to pay for idle machines (Weinhardt et al., 2009).

A considerable amount of literature has been published on the risks related to IT outsourcing. Earl (1996) discusses risks of ITO, such as the possibility of hidden costs, business uncertainty, outdated technology skills, loss of innovative capacity, and technology indivisibility. A comprehensive review of literature on ITO is published by Dibbern et al. (2004). A review of the ITO and Application Service Provision (ASP) literature is given by Lacity, Khan, and Willcocks (2009). They review 34 published papers on ITO risks and risk management and list the 28 commonly mentioned risks, including contract, security, or privacy breaches by the provider, hidden costs, lack of trust, loss of control, and vendor lock-in due to high switching costs.

So far, the focus of IS publications on ITO risks was limited to economic and management aspects, e.g., they focused on financial risks, such as hidden costs, strategic risks, such as loss of know-how, and cultural risks. According to Hahn, Doh, and Bunyaratavej (2009), IT security risks associated with IT outsourcing have not been explicitly studied.

At the same time, however, recent studies show that IT security and data privacy are the dominant factors affecting the IT executives' perceived risk of IT outsourcing (Benlian and Hess 2010). Therefore, it is an important part of IT risk management to know and understand the security risks of IT outsourcing as more and more attacks and security incidents threaten the confidentiality of intellectual property or the availability of services.

In recent years, innovative IT paradigms, such as Software-as-a-Service or Cloud Computing using third-party services, are increasingly adopted. In this context, outsourcing is getting more and more automated in order to reduce both cost and time-to-market, which results in a changeover from human relationships to human-computer interaction or even direct machine-machine interaction. Therefore, we explicitly focus on technological risks related to IT security and quality of service characteristics associated with IT outsourcing. For this reason, we exclude some risks that are associated with traditional outsourcing relationships (e.g., software development outsourcing), such as cultural risks.

This paper seeks to address the following two research questions: a) What are the technological risks of IT outsourcing? b) How can these technological risks be categorized?

Based on an extensive literature review, we create a taxonomy that covers all technological risk items related to IT security and the quality of service. As a result, nine categories of risks are described that cover all of our identified 70 risks.

The taxonomy supports IT risk management in two ways: First, the list can be used as a checklist as part of the risk identification phase and second, for all risk items found, we name the parameters that are relevant for using the taxonomy in an existing mathematical risk quantification model.

The remainder of this paper has been divided into three parts. Section 2 begins by laying out the methodology of our literature review, discussing the selection of scientific databases and keywords, describing the processes of excluding irrelevant papers, and refining the risk items and categories. In Section 3, we present the resulting taxonomy of technological risks, describe the categories, and discuss how the risk taxonomy can be applied during the IT risk management process in the phases of risk identification and risk quantification. Finally, we conclude and list possible future studies.

2 Methodology

Our literature review is based upon the approach described by vom Brocke et al. (2009). Hence, the procedure of excluding (and including) sources has to be made as transparent as possible. Moreover, the review should provide high validity and reliability in order to proof credibility.

According to Levy and Ellis (2006), *validity* is defined as the degree to which the search accurately uncovers the sources. This involves the selection of scientific databases, keywords, and journals. *Reliability* characterizes the replicability of the search process.

Cooper, Hedges and Valentine (2009) define a taxonomy of literature reviews which allows describing our methodology.

We focused on the research outcomes described or applied in the analyzed articles. Our goal was to integrate existing risk items into our work. We summarized and synthesized these items and took a neutral perspective. However, it is not possible to perform the selection of relevant risks completely neutral, as this extraction of technological risk items might be subjective to our interpretation. We tried to gain exhaustive coverage, but we were limited to those sources available for download by the seven chosen scientific databases. Our results are organized and arranged conceptually, so that works relating to the same items appear together. Our intended audience are IS researchers specialized in IT outsourcing or IT risk management, but our results might also be of value for other researchers in the IS community.

The following subsections describe our selection of sources and keywords with which we queried the databases.

2.1 Selection of Scientific Databases

For our collection of relevant publications, we used the following databases because taken together, they allow searching more than 3,000 business- and IT-related journals: EBSCOhost (with Business Source Premier and EconLit databases), ISI Web of Knowledge (with Web of Science database) and Science Direct. We excluded Wiley Online Library and ingentaconnect as their usage would not have led to an increased coverage of top IS journals.

As our goal is to collect IT-related risks, we also queried the ACM Digital Library and the IEEE Xplore Digital Library as they cover the majority of publications from computer science disciplines. The AIS Electronic Library (AISel) was used to cover the JAIS as well as the proceedings of major IS conferences like ECIS and ICIS.

This selection of scientific databases allowed searching the abstracts of 100% of the top 25 MIS journals[1] and allowed accessing the full text of 92% of these ranked publications. However, some of them were only accessible after a certain delay and eight recent papers could not be downloaded because of these embargos.

We chose to query whole scientific databases without restricting the searches to specific journals or proceedings in order to gain high coverage of all relevant sources, to be as exhaustive as possible, and to find more risks. For the same reason, the queries were not restricted to a fixed time frame. We searched all covered years and did not exclude older papers.

[1] http://ais.affiniscape.com/displaycommon.cfm?an=1&subarticlenbr=432 [2010-11-01]

2.2 Keywords

We were looking for papers in English language whose titles indicated that the publication is about IT outsourcing. Out of those, we were looking for papers that mention risk-related terms in either the title or the abstract.

The keywords were selected from the domains of IT outsourcing and IT security risks. To assure the quality of the keywords, the selection was done iteratively by sending test queries to the databases and by adding multiple synonyms and plural forms. For the terms related to IT outsourcing, we added commonly mentioned service models, and according acronyms, such as Cloud Computing, Software-as-a-Service, ASP, and SaaS. In conclusion, we queried the databases using the following keywords:

Terms related to IT Outsourcing:

((sourcing OR outsourcing OR outsource) AND (information-technology OR information-technologies OR information-system OR information-systems OR service OR services OR application OR applications OR software OR IS OR IT[2])) OR (cloud-computing OR software-as-a-service OR saas OR platform-as-a-service OR paas OR infrastructure-as-a-service OR iaas OR application-service-providing OR application-service-provider OR application-service-providers OR ASP OR netsourcing OR esourcing)

Risk-related terms:

security OR safety OR risk OR danger OR weakness OR vulnerability OR attack OR threat OR risks OR dangers OR weaknesses OR vulnerabilities OR attacks OR threats

Figure 1 provides the relations between some of the risk-related terms we used. Throughout this paper, we use the term "risk" because especially from a risk management point of view, the metrics, associated with the threats and the affected assets, are important.

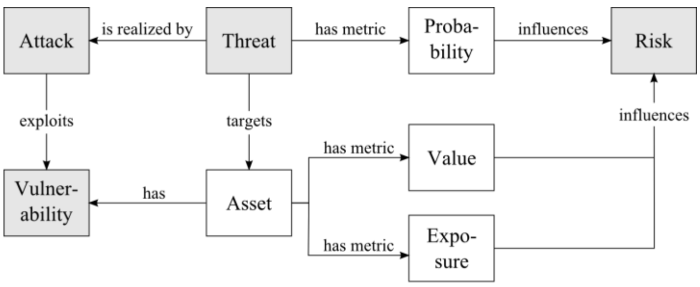

Figure 1. Relations between the risk-related terms "attack", "threat", "risk", and "vulnerability", based on Miede et al. (2010).

[2] The keywords "IS" and "IT" have only been used with scientific databases that do not treat "is" and "it" as stop words. We used hyphens whenever possible, e.g., to search for "Software-as-a-Service" as well as "Software as a Service".

2.3 Reduction of Relevant Papers through Search Filters

The search for papers with a title related to IT outsourcing and risk-related terms in title or abstract took place between May 28 and June 7, 2010, and resulted in 576 sources. Application of further search filters excluded 335 of these papers.

The resulting 241 papers identified by keyword search have subsequently been evaluated, based on their titles and other metadata, and later based on their abstracts, in order to assess their relevance for this study. 84 papers were out of scope and were therefore excluded.

Out of the remaining 157 papers, we were able to download 149. These have been evaluated based on a review of the whole content. This step resulted in exclusion of another 81 papers which were out of scope. Backward or forward searches were not part of our literature search strategy. Table 1 summarizes the steps done to reduce the number of relevant papers.

	May/28 2010	May/28 2010	May/28 2010	May/28 2010	May/28 2010	May/31 2010	Jun/07 2010	
	ACM	**EBSCO BSP**	**EBSCO EconLit**	**IEEE**	**Web of Science**	**Science Direct**	**AISel**	**Total**
A: Title is related to IT Outsourcing	105	2.220	109	612	3.542	724	70	7.382
B: Title is related to Risk	3.519	149.718	30.795	22.947	100.001	107.609	495	415.084
C: Abstract is related to Risk	12.123	589.510	56.605	83.591	n.a.	323.391	738	1.065.958
B OR C	13.122	631.609	73.403	87.307	100.001	376.688	1.122	1.283.252
A AND (B OR C)	12	267	5	84	153	50	5	576
Further Search Filters[3]	10	31	1	81	71	42	5	241
Filter By Title and other Metadata	10	31	0	81	71	42	3	238
Filter By Abstract	10	29	0	69	21	25	3	157
Papers available for Download	10	29	0	69	16	22	3	149
Review by whole Content	5	13	0	28	7	14	1	68

Table 1. The number of resulting papers after applying the search filters and after manual content filtering for each of the seven scientific databases.

Finally, the search resulted in 68 final papers, which are listed in the appendix. The period covered by all these publications is 1993 to 2010, whereas 65% of all papers found have been published between 2007 and 2010. Content analysis of the final 68 papers resulted in 757 risk items and 229 countermeasures. Due to the page limit, in the following, we focus on the risk items.

[3] We used further filters, such as searching for journals and proceedings only, papers with full text available, as well as exclusion of biology and chemistry journals.

2.4 Successive Refinement

In the following subsections, we describe the procedure used to successively refine the risk items and the taxonomy's categories. The method is comparable to the item sorting and grouping approach used by Ma et al. (2005).

2.4.1 Item Reduction

The high number of 757 initial risk items required us to reduce the number of items to a manageable set. Accordingly, as a first step, we merged items with same or similar meanings, e.g., "Poor response speed", "Low responsiveness", and "Unresponsiveness". By removing these duplicates, redundancy was reduced.

2.4.2 Regrouping of Items

In this step, we tried to cluster similar items into different categories in order to build a suitable taxonomy. We iteratively moved the risk items from one category to another and added, renamed, or removed categories. This procedure led to new categories and concepts that we initially had not anticipated.

Rarely referenced items that are subtypes of other items were also merged. For example, the items "Misuse services for sending spam" and "Misuse services for phishing", with one source each, were merged because they are more concrete instances of the item "Misuse of compromised credentials". Thereby, we decreased the items' redundancy.

The step of regrouping items was repeated multiple times. For some iterations, we invited other participants into different regrouping stages in order to achieve a gradual improvement of the clusters and to get feedback from different research backgrounds. In total, eight individuals took part in these regrouping sessions: Four IS or computer science researchers who hold a doctoral degree, three PhD students researching on IT security in the context of Cloud Computing and one IS student.

After each iteration, we made sure, that the categories are exhaustive, i.e., that all items have been assigned to a category and that there are no items that do not fit into any of the categories. Furthermore, we analyzed the categories' intra-group homogeneity, i.e., that all items of a group are similar to each other.

2.4.3 Final Grouping

As a final step, we copied the resulting 70 risk items on cards which were then randomly shuffled. Subsequently, we tried to allocate all cards to the nine identified categories. This was done in order to test if all items can be assigned to exactly one of the existing categories. By doing so, we checked whether the categories are exhaustive and mutually exclusive, and whether the classification is unambiguous.

Afterwards, we analyzed certain attributes in order to evaluate the quality of the resulting taxonomy. According to Howard and Longstaff (1998), satisfactory taxonomies have classification categories with the following six characteristics.

The taxonomy should be *exhaustive*, which means that all categories, taken together, include all the possible items. We queried seven scientific databases without restricting the searches to specific journals or time periods in order to identify as many relevant risk items as possible.

The categories should not overlap (*mutual exclusiveness*) and classification should be *unambiguous*. Our last step, the final grouping with cards, was conducted to make sure that our taxonomy is clear and precise, so that the classification is certain, regardless of who is classifying. However, small limitations were found as there were items fitting into two categories. "Service delivery problems" and "Technical issues and systems failures", for example, could be classified as "Availability" and

“Performance”. In some cases, another reason for ambiguity exists as items that could be seen as cause and effect, such as “Unsatisfactory software quality” and “Underperformance”, are grouped into different categories (reliability and performance risks).

Furthermore, repeated applications should result in the same classification, regardless of who is classifying (*repeatable*). We thoroughly documented the process of our literature review, and the intermediary steps to construct the taxonomy in order to reach high reliability. By incorporating participants with different backgrounds, we extracted categories with high intra-group homogeneity and high inter-group heterogeneity.

The taxonomy’s categories should be logical and intuitive, so that they could become generally approved and *accepted*. We used existing categories from IT security and quality of service literature and accordingly most categories are already approved by the research community.

Finally, the taxonomy should be *useful* and lead to insight into the field of inquiry. To the best of our knowledge, this paper provides the first collection and systematization of the technological risks of IT outsourcing. Additionally, in the next section, we show how the identified risk items can be practicably applied as part of the IT risk management process, in the phases of risk identification and in combination with an existing risk quantification model.

3 Taxonomy of Technological IT Outsourcing Risks

A taxonomy is a classification scheme that partitions a body of knowledge and defines the relationship of the objects (Howard and Longstaff, 1998). We created the following taxonomy of technological IT outsourcing risks in order to cluster all risk items found by our literature review. The categories are chosen to match existing classifications from IT security and quality of service literature.

Overall, the category names used for our taxonomy are a consolidation of the names used in taxonomies by Avižienis et al. (2004), Gouscos et al. (2003), and Carr et al. (1993). We extended their categories by "Accountability", because some risk items are too specific to fit into the category of "General IT Security Risks". These risks are directly related to problems with identifying responsible parties and controlling access to the systems and data (Lampson, 2009).

Categories	**#I**	**#S**	**Description**
General IT Security Risks	10	33	The three basic principles of IT security are confidentiality, integrity, and availability. Risks in this general category affect at least two of these principles. Most items name deliberate IT security attacks that can be grouped into host-based and network-based attacks.
Confidentiality Risks	5	32	Confidentiality risks include deliberate attacks that affect the privacy and confidentiality of the customer's data, such as eavesdropping communications, as well as accidental data leakage.
Integrity Risks	4	8	Integrity is compromised, whenever any unauthorized change to information in transmission or storage is involved (Amoroso, 1994). These changes range from systematic modifications to unsystematic distortion.
Availability Risks	10	37	Availability is defined as a system's ability to deliver services when requested (Sommerville, 2006). Common, deliberate methods to cause downtime are (distributed) denial of service attacks.
Performance Risks	6	35	A major concern regarding IT outsourcing is underperformance because of network issues. Other causes can be throughput problems, poor response times and limited scalability.
Accountability Risks	11	14	Accountability risks are related to the problem of identifying, authenticating, and authorizing trusted users (Schneier, 2004). Identity theft and generating costs in the name of legitimate customers are exemplary attacks.
Reliability Risks	3	27	Reliability is the extent to which a system behaves as expected by its users (Sommerville, 2006). Items include unsatisfactory software quality and insufficient accuracy of the delivered results.
Maintainability Risks	11	31	These risks can affect a system's ability to undergo modifications or repairs (Avižienis et al., 2004). This includes integration of external systems, as well as the migration from and to another provider.
Regulatory Risks	10	36	Regulatory risks include theft of intellectual property, data disclosure, or other misuse by the provider and undefined ownership of data after end of the contract or service usage.
Total	70	68	

Table 2. The nine final categories with the number of items (#I) in each category, the number of sources (#S) mentioning at least one of the items, and a brief description.

The most frequently mentioned item ("Compromised data security") shows the literature's high level focus on the topic, while only a small amount of sources name specific attacks, such as eavesdropping or distortion of data.

It is remarkable, that only a small number of sources mention integrity-related risks (8 sources) because compromised integrity, for example, due to data modifications, can indirectly lead to a breakdown and downtime of a service. Likewise, risks related to accountability (14 sources), such as missing accountability and vulnerabilities in authentication and authorization mechanisms, may be causes of other more serious risks that are related with confidentiality, integrity, and availability. Risk items of all other seven categories are mentioned by 27 to 37 sources. Furthermore, only attacks on integrity are discussed while none of the sources discusses risks caused directly by compromised integrity, such as that the data may become unusable, files cannot be opened anymore, or that specific values in transmitted data (e.g., order quantities) are manipulated which might lead to false data in the planning systems.

Compared to the other five categories, fewer risk items are mentioned related to reliability, integrity, confidentiality, and performance. This is especially the case for reliability risks, where 27 sources name only three different risk items. None of the sources describes in detail what it means when the functional quality of a service is unsatisfactory. For example, a service could return inaccurate results because it is using a heuristic for approximation instead of calculating the actual optimal value.

The IT risk management process is usually described as a procedure consisting of four phases. The first phase's goal is the *identification* of business-relevant threats. In the phase of risk *quantification*, the occurrence probability and potential losses associated with each threat are estimated. The *treatment* of risks is achieved through targeted implementation of countermeasures, while the phase of *review and evaluation* is used to evaluate the decisions made in the earlier phases (Faisst and Prokein, 2005). IT risk management is a continuous process, as the tools of the attackers, but also the available security technologies constantly evolve.

The taxonomy presented in Table 3 supports IT risk management in two ways: First, the list of technological risks can be used as a checklist as part of the risk identification phase. And second, it supports decision makers in the phase of risk quantification.

In order to support the taxonomy's usage as a checklist during risk identification, the analyzed IT outsourcing scenario has to be divided into the services it is composed of (e.g., the activities or tasks of a business process), and the data transfers which connect the services. Table 3 provides two columns next to each risk item which indicate whether or not the risk can affect services and/or data transfers. For example, "Disclosure of data by the provider" applies only to services, while "Unprotected integrity of messages" affects only data transfers. This helps to identify possible risks related to the scenario. Among the 70 risk items, 64 can be related to services and 28 can be related to data transfers.

For all risk items in the taxonomy, we also specify other parameters relevant for using them in an existing mathematical risk quantification model.

Tchankova (2002) distinguishes between hazards and perils. A hazard is a condition or circumstance that increases the chance of losses and their severity, while a peril is something which directly causes losses. The first column right to the number of sources for each risk shows whether the risk directly involves costs, i.e., whether it is a hazard or a peril. There are strong relationships between most of the identified risks, like shown in the following structure.

Compromised data confidentiality	peril	costs & probability
└── Disclosure of data by the provider	hazard	probability
└── Eavesdropping communications	hazard	probability
└── Accessing other VMs' virtual disks or memory	hazard	probability

While it is possible to estimate occurrence probabilities for hazards and perils, it is not possible to estimate the potential losses caused by hazards as only perils cause direct costs. During the phase of risk quantification, it is important to be aware of the difference between these two types of risks.

Furthermore, we marked all deliberate attacks. This is done in order to emphasize the severity of these attacks, especially when companies use recent types of IT outsourcing, such as Software-as-a-Service and Cloud Computing. In total, every second risk item can be a deliberate attack, i.e., done on purpose and in order to cause damage.

The last column of Table 3 indicates if the number of service invocations or the number of data transfers from and to a service has to be taken into account when quantifying potential losses. Some risks, such as "Incomplete contracting", are related to the provider and so the number of service calls is irrelevant, while other risks, such as "Man-in-the-Middle attacks", could occur in every single data transfer.

1. General IT-Security Risks

		#S	L	D	AS	AT	PI
1	Compromised data security	28	✓	✓	✓	✓	✓
2	Host-based attacks	9	✗	✓	✓	✗	✓
3	Malware, such as viruses and rootkits	4	✗	✓	✓	✗	✗
4	System intrusion	4	✗	✓	✓	✗	✗
5	Attacks against web services	2	✗	✓	✓	✗	✓
6	Attacks against XML	2	✗	✓	✓	✗	✓
7	Unprotected sensitive data in transmission and storage	5	✗	✗	✓	✓	✓
8	Network-based attacks	4	✗	✓	✗	✓	✓
9	Man-in-the-Middle attacks	2	✗	✓	✗	✓	✓
10	Replay attacks	2	✗	✓	✗	✓	✓

2. Confidentiality Risks

		#S	L	D	AS	AT	PI
1	Insufficient data privacy	18	✗	✗	✓	✓	✓
2	Compromised data confidentially	15	✓	✓	✓	✓	✓
3	Data leakage	12	✓	✗	✓	✓	✓
4	Attacks against confidentiality	4	✗	✓	✓	✓	✓
5	Eavesdropping communications	4	✗	✓	✗	✓	✓

3. Integrity Risks

		#S	L	D	AS	AT	PI
1	Attacks against integrity	8	✗	✓	✓	✓	✓
2	Systematic data modifications	4	✓	✓	✓	✓	✓
3	Unprotected integrity of messages	3	✗	✓	✗	✓	✓
4	Unsystematic distortion of data	2	✓	✓	✓	✓	✓

4. Availability Risks

		#S	L	D	AS	AT	PI
1	Discontinuity of the service	13	✓	✗	✓	✗	✗
2	Insufficient availability and low uptime	12	✓	✗	✓	✗	✓
3	Downtime (outages)	9	✓	✗	✓	✓	✓
4	Service delivery problems	6	✗	✗	✓	✗	✓
5	Loss of access to data	5	✓	✗	✓	✗	✗
6	Technical issues and system failures	5	✗	✗	✓	✓	✓
7	Attacks against availability	4	✗	✓	✓	✓	✓
8	(Distributed) Denial of Service	4	✗	✓	✓	✓	✓
9	Turning off the machine	1	✗	✓	✓	✗	✓
10	Data losses and insufficient recovery	4	✓	✗	✓	✗	✗

5. Performance Risks

		#S	L	D	AS	AT	PI
1	Network issues	24	✗	✗	✗	✓	✓
2	Poor response speed	7	✗	✗	✓	✗	✓
3	Throughput problems	4	✗	✓	✓	✓	✓
4	Limited scalability	11	✗	✗	✓	✗	✓
5	Deliberate underperformance and service debasement	8	✗	✓	✓	✗	✗
6	Underperformance	7	✓	✗	✓	✓	✓

6. Accountability Risks

		#S	L	D	AS	AT	PI
1	Attacks against authorization	7	✗	✓	✓	✓	✗
2	Unauthorized access	6	✗	✓	✓	✗	✗
3	Accessing other VMs' virtual disks or memory	2	✗	✓	✓	✗	✗
4	Attacks against accountability	5	✗	✓	✓	✓	✓
5	Attackers can deny performed actions	2	✗	✓	✓	✗	✓
6	Attackers generate costs in the name of legitimate clients	2	✓	✓	✓	✗	✗
7	Attacks against authentication	5	✗	✓	✓	✓	✗
8	Identity theft	5	✗	✓	✓	✓	✗
9	Misuse of compromised credentials	2	✗	✓	✓	✗	✗
10	Insufficient accountability of performed actions	3	✗	✓	✓	✓	✓
11	Insufficient separation of coexisting users	3	✗	✓	✓	✗	✗

7. Reliability Risks

		#S	L	D	AS	AT	PI
1	Unsatisfactory software quality	13	✗	✗	✓	✗	✓
2	Lack of reliability	13	✗	✗	✓	✓	✗
3	Insufficient quality and accuracy of delivered results	6	✓	✗	✓	✗	✓

8. Maintainability Risks

		#S	L	D	AS	AT	PI
1	Inflexibility regarding technological change	17	✓	✗	✓	✗	✗
2	Inflexibility regarding business change	14	✓	✗	✓	✗	✗
3	IT becomes undifferentiated commodity	8	✗	✗	✓	✗	✗
4	Incompatible systems, software and procedures	6	✗	✗	✓	✗	✗
5	Provider does not provide the tools to export data	6	✗	✗	✓	✗	✗
6	Costly modifications are necessary	4	✓	✗	✓	✗	✗
7	Insufficient maintenance and enhancements	4	✗	✗	✓	✗	✗
8	Difficult incorporation of existing data	3	✗	✗	✓	✗	✗
9	Lack of personalization functionality	3	✗	✗	✓	✗	✗
10	Service does not perfectly fit clients' needs	2	✓	✗	✓	✗	✗
11	Uncontrolled updates	2	✓	✓	✓	✗	✗

9. Regulatory Risks

		#S	L	D	AS	AT	PI
1	Theft of intellectual property	9	✓	✓	✓	✓	✓
2	Disclosure of data by the provider	7	✗	✓	✓	✗	✗
3	Misuse of data by provider	7	✗	✓	✓	✗	✗
4	Compliance risk	5	✓	✗	✓	✗	✗
5	Incomplete contracting	5	✗	✗	✓	✗	✗
6	Lack of awareness of where data is held	4	✗	✗	✓	✗	✗
7	Undefined ownership of data	3	✗	✗	✓	✗	✗
8	Breach of contract by the provider	2	✗	✓	✓	✗	✗
9	Inflexible contracts regarding changes	2	✗	✗	✓	✗	✗
10	Provider uses hidden sub-contrators	2	✗	✓	✓	✗	✗

	# Sources	Losses	Deliberate	Affects Services	Affects Transfers	Per Invocation
Legend	#S	L	D	AS	AT	PI

Table 3. *Overview of all risk categories and their items. For each item, the number of sources (#S) are given, as well as whether or not the risk can directly cause losses (L), may be a deliberate attack (D), can affect services (AS) and/or data transfers (AT) and can occur per invocation of a service or data transfer (PI).*

4 Conclusion and Future Work

The purpose of the current study was to determine the technological risks of IT outsourcing. Therefore, we conducted an extensive literature review, and thoroughly documented the process in order to reach high validity and reliability. 149 papers have been evaluated based on a review of the whole content and out of the finally relevant 68 papers, we extracted 757 risk items. Using a successive refinement approach, which involved reduction of similar items and iterative re-grouping, we created a taxonomy with nine categories for the final 70 risk items. Unlike previous research on risks of IT outsourcing, we establish a direct link of these technological risks with operational IT security and quality of service aspects. This link is especially important with respect to current types of IT outsourcing, such as Software-as-a-Service and Cloud Computing.

Moreover, we described how the taxonomy can be used to support the first two phases of the IT risk management process: Risk identification and quantification. Therefore, for each item, we gave parameters relevant for using them in an existing mathematical risk quantification model.

In order to conceptualize the construct of IT outsourcing's technological risks, a further study could carry out a quantitative approach such as the Q-sort method (Nahm et al., 2002). This would allow assessing the created taxonomy's reliability and would increase the construct's validity.

Further work needs to be done in order to extend the risk management support to the third phase, risk treatment, by showing which countermeasures help to reduce certain risks. As part of our literature review, we also collected countermeasures and grouped them into categories, such as performance management, business continuity, logging and non-repudiation, or trust and reputation establishment.

More information on the cause-and-effect chains between the identified risks and the connections to existing countermeasures would allow identifying which risks can be caused by other risks and which countermeasures protect against which risks. The associated graphs can be used in the phase of risk treatment, which could be particularly useful in the context of IT risk management decision support systems.

Acknowledgements

This work was supported by CASED (www.cased.de). The authors would like to thank Mark Bedner, Sheikh Mahbub Habib, Sebastian Kotek, Dr. Leonardo Martucci, Dr. Sebastian Ries, and Dr. Thomas Widjaja for their help with the item reduction and grouping, as well as Sebastian Kotek for his assistance on scientific database selection and item extraction.

References

Amoroso, E. G. (1994). Fundamentals of Computer Security Technology. Prentice-Hall, Englewood Cliffs, NJ, USA.

Avižienis, A.; Laprie, J.-C.; Randell, B. and Landwehr C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. In IEEE Transactions on Dependable and Secure Computing, 1 (1), 11–33.

Benlian, A. and Hess, T. (2010). The Risks of Sourcing Software as a Service: An Empirical Analysis of Adopters and Non-Adopters. In Proceedings of the 18th European Conference on Information Systems (ECIS), Pretoria (South Africa).

Butler, L. (2009). Privacy and Security: Usable Security: How to Get It. In Communications of the ACM, 52 (11), 25–27.

Carr, M. J.; Konda, S. L.; Monarch, I.; Ulrich, F. C. and Walker, C. F. (1993). Taxonomy-Based Risk Identification. Technical Report CMU/SEI-93-TR-6, Carnegie Mellon University.

Cooper, H.; Hedges, L. V. and Valentine, J. C. (2009). The Handbook of Research Synthesis and Meta-Analysis. 2nd Edition. Russell Sage Foundation, New York, NY, USA.

Dibbern, J.; Goles, T.; Hirschheim, R. and Jayatilaka, B. (2004). Information Systems Outsourcing: A Survey and Analysis of the Literature, In The Data Base for Advances in Information Systems, 35 (4), 6–102.

Earl, M. (1996). The Risks of Outsourcing IT, Sloan Management Review, 37 (3), 26–32.

Faisst, U. and Prokein, O. (2005) An Optimization Model for the Management of Security Risks in Banking Companies. In Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC), 266–273.

Gouscos, D.; Kalikakis, M. and Georgiadis, P. (2003). An Approach to Modeling Web Service QoS and Provision Price. In Proceedings of the Fourth International Conference on Web Information Systems Engineering Workshops (WISEW), 121–130.

Hahn, E. D.; Doh, J. and Bunyaratavej, K. (2009). The Evolution of Risk in Information Systems Offshoring: The Impact of Home Country Risk, Firm Learning, and Competitive Dynamics. In MIS Quarterly, 33 (3), 597–616.

Howard, J.D. and Longstaff, T. A. (1998). A Common Language for Computer Security Incidents. Technical Report SAND98-8667, Sandia National Laboratories.

Lacity, M. C.; Khan, S. A. and Willcocks, L. P. (2009). A Review of the IT outsourcing Literature: Insights for Practice, The Journal of Strategic Information Systems, 18 (3), 130–146.

Levy, Y. and Ellis, T. J. (2006) A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. In Informing Science Journal, 9, 181–212.

Ma Q.; Pearson, J.M. and Tadisin S. (2005). An Exploratory Study into Factors of Service Quality for Application Service Providers; Information & Management 42, 1067–1080.

Miede, A.; Nedyalkov, N.; Gottron, C.; König, A.; Repp, N. and Steinmetz, R. (2010). A Generic Metamodel for IT Security: Attack Modeling for Distributed Systems. In Proceedings of the Fifth International Conference on Availability, Reliability, and Security (ARES 2010), 430–437.

Nahm, A.; Solís-Galván, L. E.; Rao, S. S. and Ragu-Nathan, T. S. (2002). The Q-Sort Method: Assessing Reliability and Construct Validity of Questionnaire Items at a Pre-Testing Stage. In Journal of Modern Applied Statistical Methods, 1 (1), 114–125.

Schmitt, J. B. (2000). Heterogeneous Network Quality of Service Systems. Kluwer Academic Publishers, Norwell, MA, USA.

Schneier, B. (2004). Secrets and Lies: Digital Security in a Networked World. Wiley, Indianapolis, IN, USA.

Sommerville, I. (2006). Software Engineering. 8th edition. Addison-Wesley, Boston, MA, USA.

Tchankova, L. (2002). Risk Identification: Basic Stage in Risk Management. In Environmental Management and Health 13 (3), 290–297.

vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R. and Cleven, A. (2009). Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In Proceedings of the 17th European Conference on Information Systems (ECIS), Verona (Italy).

Weinhardt, C.; Anandasivam, A.; Blau, B.; Borissov, N.; Meinl, T.; Michalk, W. and Stößer, J. (2009). Cloud Computing: A Classification, Business Models, and Research Directions. Business & Information Systems Engineering, 5 (1), 391–399.

Appendix: Sources

This is the list of all sources considered in our literature review:

1. Altinkemer, Kernel; Chaturvedi, Alok and Gulati, Rakesh 1994. "Information systems outsourcing: Issues and evidence," International Journal of Information Management, 14 (4), 252–268.
2. Aron, Ravi; Clemons, Eric K. and Reddi, Sashi 2005. "Just Right Outsourcing: Understanding and Managing Risk," Journal of Management Information Systems, 22 (2), 37–55.
3. Bahli, Bouchaib and Rivard, Suzanne 2003. "The information technology outsourcing risk: a transaction cost and agency theory-based perspective," Journal of Information Technology, 18 (3), 211–221.
4. Bahli, Bouchaib and Rivard, Suzanne 2005. "Validating measures of information technology outsourcing risk factors," Omega, 33 (2), 175–187.
5. Baldwin, Lynne P.; Irani, Zahir and Love, Peter E. D. 2001. "Outsourcing information systems: drawing lessons from a banking case study," European Journal of Information Systems, 10 (1), 15–24.
6. Benefield, Robert 2009. "Agile Deployment: Lean Service Management and Deployment Strategies for the SaaS Enterprise," 42nd Hawaii International Conference on System Sciences (HICSS), 1–5.
7. Beulen, Erik; Fenema, Paul Van and Currie, Wendy 2005. "From Application Outsourcing to Infrastructure Management: Extending the Offshore Outsourcing Service Portfolio," European Management Journal, 23 (2), 133–144.
8. Beybutov, E. 2009. "Managing of information security with outsource service provider," International Siberian Conference on Control and Communications (SIBCON), 62–66.
9. Bhattacharya, Somnath; Behara, Ravi S. and Gundersen, David E. 2003. "Business risk perspectives on information systems outsourcing," International Journal of Accounting Information Systems, 4 (1), 75–93.
10. Briscoe, Gerard and Marinos, Alexandros 2009. "Digital ecosystems in the clouds: Towards community cloud computing," 3rd IEEE International Conference on Digital Ecosystems and Technologies (DEST), 103–108.
11. Brynjolfsson, Erik; Hofmann, Paul and Jordan, John 2010. "Cloud computing and electricity: beyond the utility model," Communications of the ACM, 53 (5), 32–34.
12. Chaves, Shirlei Aparecida; Westphall, Carlos Becker and Lamin, Flavio Rodrigo 2010. "SLA Perspective in Security Management for Cloud Computing," 6th International Conference on Networking and Services (ICNS), 212–217.
13. Chou, David C. and Chou, Amy Y. 2009. "Information systems outsourcing life cycle and risks analysis," Computer Standards & Interfaces, 31 (5), 1036–1043.
14. Currie, Wendy L. and Seltsikas, Philip 2001. "Delivering Business Critical Information Systems Though Application Service Providers: The Need for a Market Segmentation Strategy," International Journal of Innovation Management, 5 (3), 323–349.
15. Currie, Wendy L. and Seltsikas, Philip 2001. "Exploring the supply-side of IT outsourcing: evaluating the emerging role of application service providers," European Journal of Information Systems, 10 (3), 123–134.
16. Currie, Wendy L. 2003. "A knowledge-based risk assessment framework for evaluating web-enabled application outsourcing projects," International Journal of Project Management, 21 (3), 207–217.
17. Currie, Wendy L.; Michell, Vaughan and Abanishe, Oluwakemi 2008. "Knowledge process outsourcing in financial services: The vendor perspective," European Management Journal, 26 (2), 94–104.
18. Dawoud, Wesam; Takouna, Ibrahim and Meinel, Christoph 2010. "Infrastructure as a service security: Challenges and solutions," 7th International Conference on Informatics and Systems (INFOS), 1–8.
19. Dikaiakos, Marios D.; Katsaros, Dimitrios; Mehra, Pankaj; Pallis, George and Vakali, Athena 2009. "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing, 13 (5), 10–13.
20. Everett, Catherine 2009. "Cloud computing - A question of trust," Computer Fraud & Security, 6, 5–7.
21. Fowler, Alan and Jeffs, Ben 1998. "Examining Information Systems Outsourcing: a Case Study from the United Kingdom," Journal of Information Technology (Routledge, Ltd.), 13 (2), 111–126.
22. Gewald, Heiko and Dibbern, Jens 2009. "Risks and benefits of business process outsourcing: A study of transaction services in the German banking industry," Information & Management, 46 (4), 249–257.
23. Gonçalves, Vânia and Ballon, Pieter 2009. "An exploratory analysis of Software as a Service and Platform as a Service models for mobile operators," 13th International Conference on Intelligence in Next Generation Networks (ICIN), 1–4.
24. Goodman, Seymour E. and Ramer, Rob 2007. "Global Sourcing of IT Services and Information Security: Prudence Before Playing," Communications of AIS, 20, 812–823.
25. Grabarnik, Genady; Ludwig, Heiko and Shwartz, Larisa 2008. "Dynamic management of outsourced service processes QoS in a service provider - service supplier environment," 3rd IEEE/IFIP International Workshop on Business-driven IT Management (BDIM), 81–88.
26. Greengard, Samuel 2010. "Cloud Computing and Developing Nations," Communications of the ACM, 53 (5), 18–20.

27. Guah, Matthew W. and Currie, Wendy L. 2004. "Logicality of ASP in healthcare: the NHS case study," 37th Annual Hawaii International Conference on System Sciences (HICSS), 1–10.

28. Gulla, Umesh and Gupta, M. P. 2009. "Deciding Information Systems (IS) Outsourcing: A Multi-Criteria Hierarchical Approach," Vikalpa: The Journal for Decision Makers, 34 (2), 25–40.

29. Hao, Jingjing 2009. "IT outsourcing risk assessment for Chinese enterprises based on service sciences and factor analysis," IEEE International Conference on Grey Systems and Intelligent Services (GSIS), 1755–1758.

30. Itani, Wassim; Kayssi, Ayman and Chehab, Ali 2009. "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," 8th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), 711–716.

31. Jayatilaka, Bandula; Schwarz, Andrew and Hirschheim, Rudy 2003. "Determinants of ASP choice: an integrated perspective," European Journal of Information Systems, 12 (3), 210–224.

32. Jensen, Meiko; Schwenk, Jörg; Gruschka, Nils and Iacono, Luigi Lo 2009. "On Technical Security Issues in Cloud Computing," IEEE International Conference on Cloud Computing (CLOUD), 109–116.

33. Jurison, Jaak 1995. "The Role of Risk and Return in Information Technology Outsourcing Decisions," Journal of Information Technology (Routledge, Ltd.), 10 (4), 239–247.

34. Karabulut, Yuecel and Nassi, Ike 2009. "Secure Enterprise Services Consumption for SaaS Technology Platforms," 25th IEEE International Conference on Data Engineering (ICDE), 1749–1756.

35. Kaufman, Lori M. 2009. "Data Security in the World of Cloud Computing," IEEE Security Privacy, 7 (4), 61–64.

36. Kern, Thomas; Kreijger, Jeroen and Willcocks, Leslie 2002. "Exploring ASP as sourcing strategy: theoretical perspectives, propositions for practice," The Journal of Strategic Information Systems, 11 (2), 153–177.

37. Kumar, Sameer; Aquino, Edgardo C. and Anderson, Elizabeth 2007. "Application of a Process Methodology and a Strategic Decision Model for Business Process Outsourcing," Information Knowledge Systems Management, 6 (4), 323–342.

38. Lu, Yonghe and Sun, Bing 2009. "The Fitness Evaluation Model of SAAS for Enterprise Information System," IEEE International Conference on e-Business Engineering (ICEBE), 507–511.

39. Ma, Qingxiong; Pearson, J. Michael and Tadisina, Suresh 2005. "An exploratory study into factors of service quality for application service providers," Information & Management, 42 (8), 1067–1080.

40. Martinsons, Maris G. 1993. "Outsourcing information systems: A strategic partnership with risks," Long Range Planning, 26 (3), 18–25.

41. Minutoli, Giuseppe; Fazio, Maria; Paone, Maurizio and Puliafito, Antonio 2009. "Virtual business networks with Cloud Computing and virtual machines," International Conference on Ultra Modern Telecommunications Workshops (ICUMT), 1–6.

42. Mowbray, Miranda and Pearson, Siani 2009. "A client-based privacy manager for cloud computing," 4th International ICST Conference on COMmunication System softWAre and middlewaRE (COMSWARE), 1–8.

43. Nakatsu, Robbie T. and Iacovou, Charalambos L. 2009. "A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study," Information & Management, 46 (1), 57–68.

44. Ngwenyama, Ojelanki K. and Bryson, Noel 1999. "Making the information systems outsourcing decision: A transaction cost approach to analyzing outsourcing decision problems," European Journal of Operational Research, 115 (2), 351–367.

45. Oh, Wonseok; Gallivan, Michael J. and Kim, Joung W. 2006. "The Market's Perception of the Transactional Risks of Information Technology Outsourcing Announcements," Journal of Management Information Systems, 22 (4), 271–303.

46. Osei-Bryson, Kweku-Muata and Ngwenyama, Ojelanki K. 2006. "Managing risks in information systems outsourcing: An approach to analyzing outsourcing risks and structuring incentive contracts," European Journal of Operational Research, 174 (1), 245–264.

47. Patnayakuni, Ravi and Seth, Nainika 2001. "Why license when you can rent? Risks and rewards of the application service provider model," ACM SIGCPR Conference on Computer Personnel Research (SIGCPR), 182–188.

48. Qiang, Zhang and Dong, Cui 2009. "Enhance the User Data Privacy for SAAS by Separation of Data," International Conference on Information Management, Innovation Management and Industrial Engineering, 130–132.

49. Safizadeh, M. Hossein; Field, Joy M. and Ritzman, Larry P. 2008. "Sourcing practices and boundaries of the firm in the financial services industry," Strategic Management Journal, 29 (1), 79–91.

50. Schwarz, Andrew; Jayatilaka, Bandula; Hirschheim, Rudy and Goles, Tim 2009. "A Conjoint Approach to Understanding IT Application Services Outsourcing," Journal of the AIS, 10 (10), 748–781.

51. Viega, John 2009. "Cloud Computing and the Common Man," Computer, 42 (8), 106–108.

52. Vitharana, Padmal and Dharwadkar, Ravi 2007. "Information Systems Outsourcing: Linking Transaction Cost and Institutional Theories," Communications of the AIS, 20, 346–370.

53. Walsh, Kenneth R. 2003. "Analyzing the Application ASP Concept: Technologies, Economies, and Strategies," Communications of the ACM, 46 (8), 103–107.

54. Wang, Jian; Zhao, Yan; Jiang, Shuo and Le, Jiajin 2009. "Providing privacy preserving in cloud computing," International Conference on Test and Measurement (ICTM), 213–216.

55. Wang, Cong; Wang, Qian; Ren, Kui and Lou, Wenjing 2009. "Ensuring data storage security in Cloud Computing," 17th International Workshop on Quality of Service (IWQoS), 1–9.

56. Wang, Cong; Wang, Qian; Ren, Kui and Lou, Wenjing 2010. "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," 29th IEEE International Conference on Computer Communications (INFOCOM), 1–9.

57. Wang, Hui 2010. "Privacy-Preserving Data Sharing in Cloud Computing," Journal of Computer Science and Technology, 25 (3), 401–414.

58. Willcocks, Leslie P. and Lacity, Mary C. 1999. "IT Outsourcing in Insurance Services: Risk, Creative Contracting and Business Advantage," Information Systems Journal, 9 (3), 163–180.

59. Xiong, Li; Chitti, Subramanyam and Liu, Ling 2007. "Preserving data privacy in outsourcing data aggregation services," ACM Transactions on Internet Technology, 7 (3), Article 17.

60. Xu, Jing; Jinglei, Tang; Dongjian, He and Yang, Zhang 2009. "Security Scheme for Sensitive Data in Management-Type SaaS," International Conference on Information Management, Innovation Management and Industrial Engineering, 47–50.

61. Yalaho, Anicet and Nahar, Nazmun 2008. "Risk management in offshore outsourcing of software production using the ICT-supported unified process model: A cross-case study," Portland International Conference on Management of Engineering Technology (PICMET), 1721–1748.

62. Yildiz, Mehmet; Abawajy, Jemal; Ercan, Tuncay and Bernoth, Andrew 2009. "A Layered Security Approach for Cloud Computing Infrastructure," 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), 763–767.

63. Ying, Wenlan; Li, Aiping and Xu, Liyun 2008. "Research on the authentication strategy of ASP mode-based networked manufacturing system," IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM), 1014–1017.

64. Young, Peter C. and Hood, John 2003. "Risk and the Outsourcing of Risk Management Services: The Case of Claims Management," Public Budgeting & Finance, 23 (3), 109–119.

65. Yu, Shucheng; Wang, Cong; Ren, Kui and Lou, Wenjing 2010. "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," 29th IEEE International Conference on Computer Communications (INFOCOM), 1–9.

66. Zhang, Xinwen; Schiffman, Joshua; Gibbs, Simon; Kunjithapatham, Anugeetha and Jeong, Sangoh 2009. "Securing elastic applications on mobile devices for cloud computing," ACM workshop on Cloud Computing Security (CCSW), 127–134.

67. Zhang, Yue and Shi, Xiaojun 2009. "Offshore Software Outsourcing Risk Evaluation: An Experimental Approach Based on Linear Mixed Model," 6th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 505–509.

68. Zhou, Linzhen; Liu, Defang and Wang, Bin 2008. "Research on ASP-Based Information Security System," International Symposium on Computer Science and Computational Technology (ISCSCT), 746–749.